ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research -GRANTHAALAYAH
January 2021, Vol 9(1), 202 – 210
DOI: https://doi.org/10.29121/granthaalayah.v9.i1.2021.2981

HUMAN FACTORS AFFECTING DIGITAL SECURITY

Avijit Dutta *1 ✉

*1 Ex-Scientist F, NIC, New Delhi, India

DOI: https://doi.org/10.29121/granthaalayah.v9.i1.2021.2981

Article Type: Research Article

Article Citation: Avijit Dutta. (2021). HUMAN FACTORS AFFECTING DIGITAL SECURITY. International Journal of Research - GRANTHAALAYAH, 9(1), 202-210. https://doi.org/10.29121/granthaalayah.v9.i1.2021.2981

Received Date: 03 January 2021

Accepted Date: 31 January 2021

Keywords:
Cryptography
Certifying Authority (CA)
Collective Intelligence
Digital Signature
Digital Signature Certificate (DSC)
Encryption
HDI
NCSI

ABSTRACT

World is getting digital at an exponential rate. Commonplace activities are accomplished increasingly over digital platform to bring in requirement of digital security in place of only physical security. Security (physical or digital or both) is essential for safe storage, retrieval and exchange of physical or digital data and documents. As data/information/knowledge leading to wisdom are increasingly getting endowed with economic values the risk for such assets being pilfered are also increasing. This requires methods for their security being augmented continuously. Society from past to present days are putting their best efforts in this end. Generally, it is achieved through hiding the message from predator's greedy glare and ensuring its temper-free safe passage to desired destination with deception in various forms. Associated processes are complex and during initial days were executed with various forms of arts and riddles. Over years technology driven solutions were evolved to ensure today's digital security requirements [7],[8].

Motivation/Background: Presently occurrence of digital security disasters is not few and far between, instead they are alarmingly many, though technology for digital security is improving by leaps and bounds. More often than not, in case of a digital catastrophe dominant foot prints of human involvement are found along with technical snags. It may be noted that technical failure can be assessed and rectified in an organized way though causes of human involvement are difficult to judge as they are much abstract in nature and difficult to measure. Thus, this effort to explore human role in digital disaster.

Method: In present text traditional to most current practices of securing data storage, retrieval and disbursal are touched upon. During earlier days data hiding technique from predator's glare had been more of an artistic than scientific form. Over years mathematical and statistical approach were induced to make the system more robust though secrets are exposed even today at an alarming rate and at times by their own creators to usher security disasters. As the discussion progressed results from secondary sources are presented to make a broad statement on current scenario. Finally, indicators like NCSI (National Cyber Security Index) and DDL (Digital Development Level) from NCSI site and HDI (Human Development Index) from Human Development Report of 2019, produced by UNDP, are considered for analysis to have better insight. These figures are available on public domain for general referral [24],[25].

Results: It has been observed that beyond technical complications, human factors play a dominant role in ensuring security.

1. INTRODUCTION

As the world is getting increasingly digital, security consideration too is getting associated to digital perspective along with other related issues. Message exchange in different forms, business communications, transportations, financial activities, industrial operations, medical activities etc. all are getting aboard digital platform. As such related security operations too followed the trend, which is expected to be leaner, thinner and smarter. In most scenario security features are implemented elaborately over all activity components, nevertheless breaches occur in alarming frequency, more often than not also due to human lapses. There are many instances of successful cyber-attacks and subsequent system takeover by predator that led to institutional and national fallout, raising question on the security system's efficacy. In the ensuing analysis on failure, generally attempts are made to find out whether the catastrophe is due to failure of digital system or led by inappropriate handling by ignorant users. Technical cause of digital system failure can be detected, gauged, rectified and improved, however assessment of failure resulted out of human system is not easy as it comprises of many non-measurable abstract attributes. In the present text a window view on existing technology, evolution of security & defense mechanism and possibilities of human lapses are discussed to ascertain future course [4], [7], [8].

2. HUMAN INTEGRATION WITH TECHNOLOGY

Evolution of technology, their standardization and convergence lead to nomadic and ubiquitous computing as presumed by Mark Weiser at the beginning of this century. He talked about 'profound technologies', which would be widely used to get assimilated with our day-to-day life indistinguishably, in a way to become indispensable part of larger social processes [15], [16]. ICT (Information and Communication Technology) is one such technology that has become intimate part of our living processes. As humanity is moving towards information society, riding on nomadic and ubiquitous computing with ever mounting Computing and Communicating (C&C) strength, internet access is growing exponentially.

It is assumed by leading scientists [14], [15] that internet is growing like any living entity from a state of infancy to maturity to attain a state of collective intelligence, which will be evolving continuously and available to all, evenly. Innumerable devices with sensors for seeing, listening, recording and at times analyzing abilities that people do carry during their daily activities are working as sensory organs of internet to collect and analyze information from all form of sources to amass knowledge that may lead to ultimate Wisdom.

Internet in this process has evolved from new born Web 1.0 (Static Web) to more maturing one like Web 2.0 (Dynamic and Interactive Web) and marching onwards possibly to Web 3.0 (or Web Square!), to a state of collective intelligence. Now access to C&C devices are not limited to selected elites, instead it got more democratized and has come to doorstep of commoners. Growing types of devices and connectivity options with defined standards and protocols are allowing inter and intra device connectivity, switching client and server role as and when scenario demands [12], [14]. This progressed further to many-to-many connectivity environment, overlapping people and C&C devices from different origin. Today's INTERNET works on three tire architecture as shown in Figure 1.

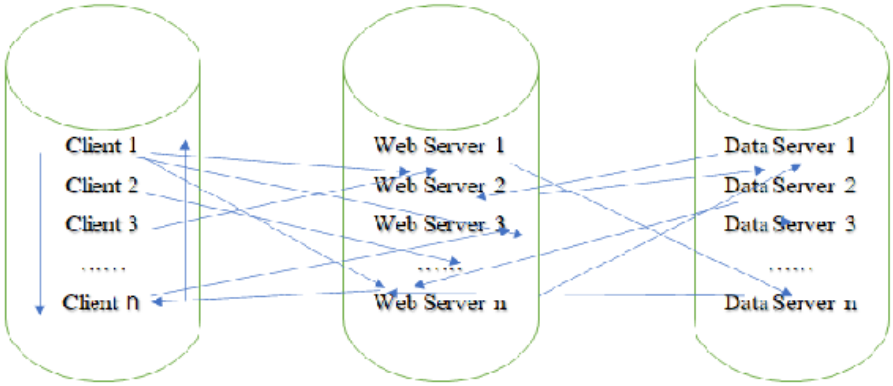

Figure 1

The vast pool of information with servers all across the world, possesses immense economic value in both black and white market. Some seeks access to it for more analysis and value addition even with some financial expenses. Others may not have any interest in their present worth, financial or otherwise, they simply intend to Gatecrash and look for onward selling scope for quick monetary gains. Security arrangements are more important to throttle this kind of predators who look around for unauthorized access to valued resources. Sometimes even casual web surfers too cause unintended security breaches both at client and server systems, that leads to major catastrophe. It may be noted here that all people who come on board (internet), uses common tools with different intentions. This raises a common concern for security amongst netizens. As a result, the scare, 'Who is on other side of wire', is growing, which calls for deeper attention on insecurity from unknown sources. This brings in the necessity to discuss digital security provisions in light of Authentication & Authorization, Data Hiding and Safe information Transmission as listed below.

1) Authentication and Authorization
2) Information Hiding (data encryption) from predators
   and
3) Safe information transmission amongst genuine senders and receivers simply with message hashing or with digital signature.

This in turn brings in the necessity to deliberate on subject cryptography, which traditionally and currently had been helping us to meet the indicated requirement.

3. AUTHENTICATION AND AUTHORIZATION

The process of physical or digital security starts with authentication and then authorization provided by the authenticating agency. It is quite in common place that security guard in an establishment stops any individual seeking entry and demands for identity establishment and then the authorizing entity allows the stranger for certain activities/interactions with system. Apart from resource protection and preservation, activities of Authentication and Authorization is everywhere in place as a first layer of defense, from physical to digital form of institutions all alike [13].

Large server clusters world over are also regarded like institutions that houses specific services and caters to various human needs similar to any other medical, technical, academic and research organizations that exists physically. In fact, now knowledge resources of most prestigious establishments are digitized and stored on internal or external servers or cloud storage for general access and common good. These resources need to be protected, with authentication and authorization tool as first line of defense. Not all such resources are there for free access, restrictions are applied on some information sets related to economic, social, technical, industrial, scientific, medical, political, defense etc. related affairs. Even, there are different price tags for different sets of information to access. Authentication and Authorization services comes into play with varied complexity in such instances to ensure protection of information wealth in line with laid down norms. This is the first hop when an intended user attempts to enter a resource center, physical or digital. Access permission is granted when the user presents evidences on identity and authenticity, based either on 'Knowledge 'or 'Possession 'or 'Inherence' or 'Location' or in combination of the stated factors, to gain entree to resource base.

In its simplest form at first identification proof is requested then the visitor is asked for a passphrase, which is not sharable. It may be mentioned here that pass phrase that is generated out of user-controlled information as mentioned earlier, can be multi layered. Depending on its layers we design single to multi factor authentication scheme.

The number of evidences demanded can stretch from one to many, which can be termed as 'Single Factor (1FA)', 'Two Factor (2FA)', 'Three Factor (3FA)' and so on, comprising of many factors like 'Multi Factor (MFA)' based authentication. In single factor, a user generally needs to submit 'user identification' which is in his possession and 'password' which user generates out of his knowledge.

In two factor (2FA) authentication system, two distinct form of identification of users are required to gain access and proceed further in the process. The first factor generally is a password, which essentially is in user's possession and the second one commonly includes a text with a code sent to user's smartphone or biometrics using user's face,

retina or fingerprint, ensuring users unique identification. Though not completely full proof, 2FA improves security to a great extent.

In order to improve security further, more than two pieces of evidences may be demanded by a system, which takes a user to Multi-factor authentication method, in which a user is granted access to resources only after successfully presenting all required pieces of evidence (or factors) to an authentication mechanism.

It may be noted that these factors/evidences are not sharable. If shared, authenticating factors gets compromised opening access for unlawful users, which may lead to a catastrophe. After being authenticated and authorized for system access, user may face encrypted resources, which may need further knowledge for decryption and data verification with hash functions. This brings us to cryptographic concepts which is touched in the following section [13, 20].

4. DATA HIDING AND CRYPTOGRAPHY (CLASSICAL AND MODERN)

In the context of data hiding, the issues of cryptography, both in classical and modern forms find a place for reference. Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing." Historically (say, before the 1980s), it was considered broadly as a form of art and achieved through process of substitution associated with secret codes, set of information and instructions.

Innumerable traditional cryptographic specimens/notes exist in social and religious practices. In ancient manuscripts these existed at places like center of pages, in margins or colophons, as acrostics, as solutions to riddles, as glosses etc. It may also be in the language of the text or in the reader's language if that is different or in scribal notes and at times as examples in descriptive areas on practice and purpose of cryptography itself. Many wealth centers had been discovered after cracking such notes.

Since earlier years ‘replacement’ remained core technique in cryptography for information protection and hiding and mostly military and intelligence establishments had been major users of it. Gradually more mathematical algorithms got into play to enhance security, as can be seen in role and functions of German Enigma Machine, in secret message exchanges during world war II.

Progressively replacement processes made way for randomized methods and in the late 20th century, the picture of cryptography changed radically with advanced mathematical and statistical derivations. Steadily it evolved as an area of both pure and applied science. Rich theories emerged enabling rigorous scientific study of cryptography. The field presently incorporates much more than mere secret communication. Now, it includes capabilities like message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, etc. with wide range of applicability, making it a ubiquitous tool for data protection.

Modern cryptography can be said to be concerned with problems that may arise in any distributed computation, which may come under internal or external attack. One may say it is the scientific study of techniques for securing digital information, transactions, and distributed computations. Over a period of time these mechanisms are standardized and abstracted with encapsulation of procedural complexities so that commoners can use them easily to remain safe. Digital security mechanism that counts on cryptography, is an integral part of almost any computer system now. Users (often unknowingly) rely on cryptography every time they access a secured website. However, unabated and frequent cyber-attacks with successful intrusion at times underlines inadequacy of existing mechanism. [7], [8].

Cryptography is also used to implement access control in multi-user operating systems, and to prevent thieves/eves droppers from extracting inclement secrets from stolen systems. Software protection methods employ encryption, authentication, and other tools to prevent illicit copying. The list of benefits from cryptography are many. However, Allan Turing, an English mathematician and computer scientist observed that not all mathematical/statistical solution for a real-life problem, even an excellent one, can be coded in a computer system. This indicates limitations of present advanced randomized mathematical cryptographic approaches.

In following sections attempt is made to elaborate more technical aspects of digital security requirements like Authentication and Authorization, Network Communication, Cryptography & Crypto Analysis etc. leading to an analysis to assess whether or not human lapses defeat scientific approach! While Technical protection generally appears to be complete, comprehensive and up-to-date, human factors remains dubious issue.

5. APPLICATION OF MODERN CRYPTOGRAPHY PKI (PUBLIC KEY INFRA STRUCTURE)

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents being send or received over internet. Digital signatures are a standard element of most cryptographic protocol suites and are commonly used for digitally exchanging documents that needs safety, security and integrity. It employs both symmetric and asymmetric cryptography. In symmetric cryptography a single key is used for cryptographic applications. In asymmetric cryptography a 'KeyPair', consisting of mathematically related a 'Private Key' and a 'Public Key', plays central role, doing most of designated operations like Data Signing, Data Verification, Data Encryption and Data Decryption. It provides layers of validation and security to messages sent and received over digital channel. It provides non-repudiation feature too, where in the signers cannot successfully claim that they have not sent the message [9].

To add further legitimacy third party authentication is applied through Certifying Authorities (CA), approved by designated CCA (Controller of Certifying Authorities). CA provides Digital Signature Certificates (DSC) to Individuals, Computer Servers as Individuals and to Institutions for various purposes under different classifications [2], [18].

It is important to note that in PKI environment, implementing asymmetric cryptography, where Public Key is for sharing though Private Key is supposed to remain strictly private. If in case Private Key gets exposed to one who is not real user/holder, the 'KeyPair' or Key is stated to be compromised and becomes invalid for cryptographic applications. This may also lead to legal liability. A valid digital signature, where the requisites are satisfied, establishes authenticity of a message send to a receiver and provides assurance that message received not tempered on transit. In this way it provides both Authenticity, Integrity and non-repudiation. Some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature remains valid.

6. SECURED DATA TRANSMISSION OVER INTERNET

Present days ICT (Information and Communication Technology) applications run on three tire architecture as shown in Fig-2, where client request is forwarded to data/information server and desired response received from it through a Web/Application Server following HTTP (Hyper Text Transfer) Protocol. Technology dependent authentication and authorization process are applied to ensure security at different layers, starting with Client, Business Logic and Database Tire.

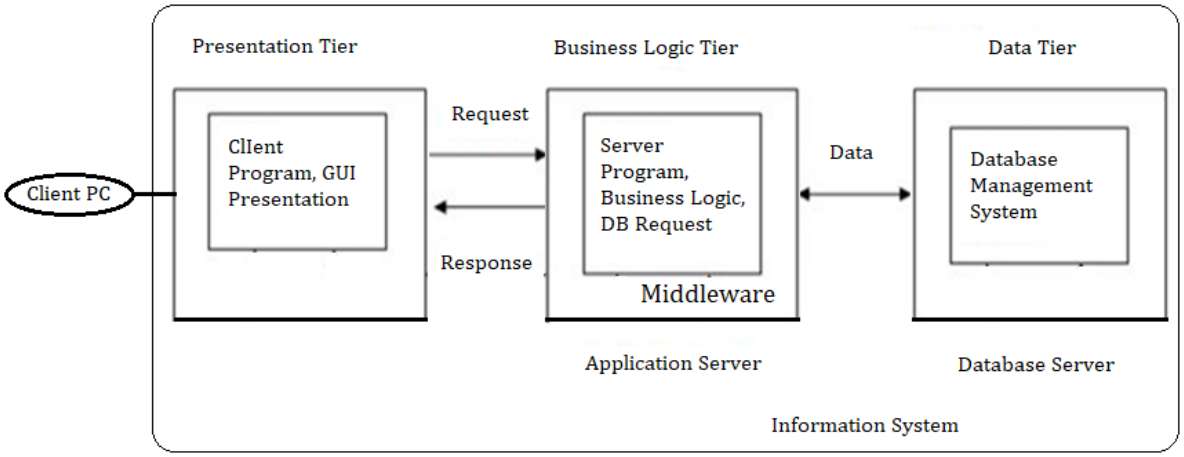

Figure 2

A secured hypertext transfer protocol; HTTPS is security induced protocol involving PKI (Public Key Infrastructure) standards, where in 'DSC' is installed on web servers to provide server identification so that the clients accessing them be assured that they are accessing the desired server. In this archetype data/information is send and received in encrypted form. HTTPS is achieved through SSL (Secured Socket Layer) or more advanced TLS (Transport Layer Security) protocol. Web site addresses adhering to this protocol precedes with a lock icon, as shown below in figure 3 –

Figure 3

A click on the icon provides necessary page information, which includes details of digital certificate, its validity, certificate issuer (the CA), subject (certificate receiver), public key, signature algorithm hashing algorithm etc. It authenticates server with which client system attempts to establishes connection and ensures safe message exchange (in signed and encrypted form) with it. Present days computing is generally executed over internet where in PKI ensures safety and security.

Thus, requirement for data/information/knowledge safety and security and protected message exchange took us from artistic replacement approach followed in classical or medieval cryptography to modern cryptography based on randomized procedure evolved out of mathematical/statistical algorithms. At the center of present procedure is Cryptographic Key (Symmetric or Asymmetric), which makes the cyphering system quite robust [11],[14].

It may be noted that, despite all standards and specifications followed by PKI processes, Certifying Authorities (CA), the identity and security providers don't always work in unison. Digital Signature Certificate (DSC) provided by one CA may or may not be recognized by others, giving a feeling of insecurity amongst PKI users and security seekers.

7. CRYPTOANALYSIS

The process to study and explore the ways to break the crypto system is known as Cryptanalysis. The word Cryptoanalysis is made out of Greek word 'kryptós', "hidden", and 'analýein', "to loosen" or "to untie". It is the study and analyzing of an information system to explore hidden aspects in it. In present order to break the cypher system a predator/eves dropper primarily need to have access of the key, which is at the core of entire process. The cryptographic key allows one to completely break into the system and have a comprehensive view. Alternatively, various guess works comes into play, which can be resource and time driven. Cryptoanalysis methods are used to crack the cryptographic security system and gain access to encrypted message even if cryptographic key is unknown. However, this activity will also need computational resource in following terms

- **Data –** about plain and cypher text to ascertain requisite approach,
- **Memory –** to compute for deciphering the cyphering the system,
- **Time -** to execute requisite steps (test encryption) to be performed,

The process is complex as it needs knowledge of many factors like internal information, key-length, key-algorithm, encryption algorithm, signing algorithm etc. These apart given some ciphertext/encrypted data the goal of a cryptanalyst is to gain as much information as possible about the original plaintext/unencrypted data. Attack types also can be classified depending on information available with attacker. Cryptoanalysis evolved with cryptography. The contest amidst cryptography and cryptoanalysis can be traced in the history of cryptography. New cyphering techniques are evolved continuously to replace old ones to make system more robust, so also new cryptanalytic techniques developed to break new schemes. They are viewed as two sides of same coin [2], [11], [21].

8. HUMAN ROLE

It is not crypto analysis always that enables a predator to break a cryptographic scheme alone, improper handling of secrets, insincerity or lack of user awareness exposes cryptographic secrets. Apart from technical, human factor plays great role in maintaining or breaking cryptographic system. Episode involving Edward Snowden who illegally used co-worker's security details to access high security server data and made the same public, points to this fact substantially. Frequent warnings in all forms of media, both print or digital, to stay away from unlawful websites, unsolicited telephone calls and email/messages from unknown sources, generally goes in vain. Often circulated advisories not to share OTP, PIN, passwords, personal information etc. with strangers also gets less than desired attention. These are attempts by predators to break into the system and steal resources. End users need to

be cautious as a single security mistake may lead to a disaster that no technology can defend. Apart from individual affect, attempt for security breach can be institutionalized by a group or even by a country. Such attempts can endanger industry, infrastructure, economy and even national security. As such care is needed while seeking external assistance and engaging exterior contractors. In these perspectives human factors like awareness, alertness, resolve with sincerity to system matters a lot to make digital security successful.

9. ANALYSIS OF FACTS

Leading computer system manufacturer DELL has conducted a survey to assess how in an institution employee keep up with security policy of the institution while sharing files and documents with external agencies during business. It has found that around 41% employees likely to bypass institution's security policy and 57% finds that this is the best way get the job done fast. 43% Employees send work related email from their personal account. Around 71% of employees share files with third parties, from outside the institution. Obviously, role of technologies is minimal in such environment and system opens up to attackers.

In its study report a California bases private company 'Netwrix', which develops change management software to help institution with compliance and auditing, found in 2020 pandemic situation vulnerability increased by 60 % when work from home become new normal for all ICT institution and 63 % increase in cyber-attack. 58% institutions have observed that employees working from remote are not adhering to institutional norms of cybersecurity. This may occur out of ignorance bordering to negligence too. Organizations are also concerned about vulnerability arising out of VPN exploitation, cloud misconfiguration and most interestingly about data theft by their own employees [5].

It is evident that possibilities for successful attacks are many thus a broad perspective is necessary which may lead to a measure that may reflect on digital security issues. In this context three measures available in public domain are considered for further deliberation, are as follows-

1) National Cyber Security Index (NCSI)
2) Digital Development Index (DDL)
3) Human Development Index (HDI)

To take the discussion further these parameters need an introduction at this juncture. To begin with let us talk about cyber security data of countries, available as National Cyber Security Index (NCSI), which is evolved and sustained by e-Governance Academy Foundation. NCSI is a global index, known as a measure to indicate preparedness of countries to prevent cyber threat. The data held by NCSI is publicly available and is a tool for cyber security capacity building endeavor. NCSI also presents Digital Development Level (DDL) and difference between these two indices. A positive difference between NCSI and DDL indicates Cyber Security Preparedness is more than Digital Development level. A negative difference indicates the digital development level is not completely exploited for Cyber Security Preparedness [25]. From the same site, latest data of top twenty NCSI scoring nations are considered along with their Digital Development Level (DDL)for further insight into the relation between 'National Cyber Security' and 'Digital Development'. This apart, top twenty NCSI scoring nations data were compared with related countries latest Human Development Indices (HDI), prepared by United Nations under United Nations Development Program (UNDP) to explore how human factor affects cyber security, in keeping with the essence of present text[24],[25]. The result of the study is tabled below,

Table 1

Measures	NCSI	DDL	HDI
Mean	82.73	75.5	0.893
Median	81.82	78.34	0.892
Mode	81.82	NA	0.891
Standard Deviation	5.915306	7.891234	0.043067
Coefficient of Variation	0.071504	0.104526	0.048267
Correlation NCSI vs DDL	-0.15037		
Correlation NCSI vs HDI	0.045172		
Correlation DDL vs HDI	0.880219		

10. DISCUSSION AND CONCLUSION

Looking at the result derived out of the data considered for analysis following observation can be made,

1) NCSI (National Cyber Security Index) of top twenty countries observed to have Statistical Mean close to median and mode value and low standard deviation and coefficient of variation, which may indicate that top twenty NCSI indexed countries follow a very uniform cyber security protocol.
2) Result derived out of DDL (Digital Development Level Index), of top twenty NCSI indexed countries also shows healthy central tendency with low level of data dispersion, which may be due to their almost equivalent level of Digital Development Environment.
3) HDI (Human Development Index), prepared by United Nation Development Program (UNDP), in the year 2019 of top 20 NCSI countries observed to have strong central tendency and low measures of dispersion, indicating almost equivalent level of human development processes as reflected collectively by measures like life expectancy, mean and expected years of schooling, gross national income etc.
4) Positive Correlation has been observed between DDL and NCSI and strong Correlation has been observed DDL and HDI.

The observations above in general and at no '4' in particular, indicates importance of human development in terms of education, physical and financial health to ensure digital security. The discussions above strongly underline role of humans in the process of ensuring digital security. As stated generally it is the man behind the machine that matters most. Many digital disasters originate from acts of human ignorance, obliviousness, violence of norms, conscious avoidance of standard operational procedures etc. which fails scientific fortification of resources. This calls for elevation of human quality with literacy, health, availability of resources and conscious access and utilization of digital resources

11. RECOMMENDATIONS

Human Development with education, health and financial upliftment improves understanding of ICT (Information and Communication Technology) and its use for community progression, which likely to ensure more secure digital environment.

SOURCES OF FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

The author have declared that no competing interests exist.

ACKNOWLEDGMENT

I acknowledge numerous ICT researchers and philosophers who immensely contributed to the subject and integrated other areas of studies that made conceptualization of this text possible.

REFERENCES

[1] Angsuman Das, Avishek Adhikari, On Constructions and Security Notions of Public-key Cryptosystems; Book Chapter, Contemporary Topics in Mathematics and Statistics with Applications, Volume-I, Asian Books Pvt Ltd., 2012; academia.edu/2904162
[2] B. Preneel et al, New Trends in Cryptology, Document Reference ENS-D4-1.1, Version 1.1, February 21, 2003
[3] Benjamin A. Saltzman Early Medieval Cryptography, Textual Errors, and Scribal Agency; SPECULUM; A journal of Medieval Studies

[4] Cortada J. W, Gupta A.M. Le Noir Marc; How Nations thrive in the Information Age, IBM Institute for Business Value, IBM Global Business Services,
[5] Cyber Threats Report, Netwrix; 2020;
[6] DELL, "Evolving Security to Accommodate the Modern Worker" Statistics based on a study conducted by Forrester Consulting commissioned by Dell, "," October 2017.
[7] Dutta Avijit, Digital Security: An Enigma, Springer Nature Singapore Pte Ltd. 2018, M. U. Bokhari et al. (eds.), Cyber Security, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_25.
[8] Dutta Avijit; Digital Security: A Moving Target, International Journal of Electrical Electronics & Computer Science Engineering Special Issue - TeLMISR 2015, ISSN, ISSN: 2348-2273,
[9] Jonathan Katz and Yehuda Lindell; Introduction to Modern Cryptography; Book; 2007
[10] Karlene C.Cousinsa, DanielRobeyb; Human agency in a wireless world: Patterns of technology use in nomadic computing environments; Information and Organization; Volume 15, Issue 2, April 2005, Pages 151-180
[11] Matthew K. Franklin, Lucas Chi Kwong Hui, Duncan S.Wong (Eds.), Cryptology and Network Security, 7th International Conference, CANS 2008, Hong-Kong, China, December 2-4, 2008, Proceedings
[12] Ruth M Davis, Evolution of Computers and Computing, Science Vol. 195; Science 18 Mar 1977: Vol. 195, Issue 4283, pp. 1096-1102; DOI: 10.1126/science.195.4283.1096
[13] The Role of Access Control in Information Security - Hashed Out by The SSL Store; 11/14/2020
[14] Tim O'Reilly and John Battelle; Web Squared: Web 2.0 Five Years On; Special Report
[15] Weiser, M.; The Computer for the 21st Century, Scientific American, September 1991, Pages 94-104
[16] Weiser Mark and John Seely Brown; THE COMING AGE OF CALM TECHNOLOGY; Xerox PARC, October 5, 1996
[17] https://notes.shichao.io/cnspp/ch2/#encryption-requirements
[18] https://en.wikipedia.org/wiki/Digital_signature
[19] https://en.wikipedia.org/wiki/Public_key_infrastructure
[20] https://en.wikipedia.org/wiki/Multi-factor_authentication
[21] https://en.wikipedia.org/wiki/Cryptanalysis
[22] https://en.wikipedia.org/wiki/Brute-force_attack
[23] https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/shift-cipher
[24] http://hdr.undp.org/en/2019-report/download
[25] https://ncsi.ega.ee/ncsi-index/.